# INTERNET, EMAIL AND INSTANT MESSAGE SAFETY TIPS

Dear Parents & Guardians,

I am writing to share with you incidents that we've experienced and to solicit your help in securing your child's safety via the Internet, email, and instant messaging via personal computers, cell phones and sidekicks. Most of the information in this letter comes from the National Center for Missing and Exploited Children.

"Cyberspace," the "Web," the "Net," the "Information Highway" — Millions of people are now going online to exchange electronic mail (E-mail) and instant messages (IMs); participate in chat groups; post and read messages in newsgroups, which are sometimes called bulletin boards; "surf" the world wide web; and many other online activities. <u>Children</u> are no exception, in fact they <u>are more likely to be online than adults</u>.

Personal computers are no longer the only method used for accessing the Internet. Children can go online from personal computers at home, a friend's house, in school, a library, club, or cafe. Even game consoles can be connected to the Internet and used for chatting and other online interaction. It is also possible to access the Internet on mobile devices such as cellular telephones, palm pilots, sidekicks, blackberries and other handheld devices. In other words children don't have to be in the company of responsible adults to use the Internet.

There are no censors on the Internet. Anyone in the world — companies, governments, organizations, and individuals — can publish material on the Internet. An Internet Service Provider (ISP) links you to sites, but it can't control what is on them. It's up to individuals to make sure that they behave in a way that's safe and appropriate.

We must work together to ensure that our children are made aware of the potential danger in communicating via the Internet. Most people who go online have mainly positive experiences. But, like any endeavor, there are some risks and annoyances. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitative. Children get a lot of benefit from being online, but they can also be targets of crime, exploitation, and harassment in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children need parental supervision and common-sense advice on how to be sure that their experiences in "cyberspace" are happy, healthy, and productive.

Teenagers are particularly at risk because they often go online unsupervised and are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity.

**Some risks are:**

- **Exposure to Inappropriate Material**

1

A child may be exposed to inappropriate material that is sexual, hateful, or violent in nature, or encourages activities that are dangerous or illegal. Children could seek out such material but may also come across it on the web via chat areas, E-mail, or instant messaging even if they're not looking for it.

- **Physical Molestation**

  A child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In some cases child molesters have used chat areas, E-mail, and instant messages to gain a child's confidence and then arrange a face-to-face meeting.

- **Harassment and Bullying**

  A child might encounter messages via chat, E-mail, or their cellular telephones and sidekicks or blackberries that are belligerent, demeaning, or harassing. "Bullies," typically other young people, often use the Internet to bother their victims.

- **Viruses and Hackers**

  A child could download a file containing a virus that could damage the computer or increase the risk of a "hacker" gaining remote access to the computer; jeopardizing the family's privacy; and, perhaps, jeopardizing the family's safety.

- **Legal and Financial**

  A child could do something that has negative legal or financial consequences such as giving out a parent's credit-card number or committing to an online purchase.

## How Parents Can Reduce the Risks

While children need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the "real world" also apply while online. If you have cause for concern about your child's online activities, talk to them. Also seek out the advice and counsel of teachers, librarians, and other Internet and online service users in your area.

Having open communication with your children, using computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use.

If your child tells you about an upsetting message, person, or web site encountered while online, don't blame your child but help him or her avoid problems in the future. Remember — how you respond will determine whether they confide in you the next time they encounter a problem and how they learn to deal with problems on their own.

Beyond these basics, there are some specific things that you should know about the Internet. For instance did you know that there are chat areas, newsgroups, and web sites that have material

that is hateful, is violent, or contains other types of material that parents might consider to be inappropriate for their children? It's possible for children to stumble across this type of material when doing a search using one of the web sites that is specifically designed to help people find information on the Internet. Most of these sites, called "search engines," do not, by default, filter out material that might be inappropriate for children, but some offer a childsafe option and some are designed specifically for use by children.

Also the Internet contains newsgroups, web sites, and other areas designed specifically for adults who wish to post, read, or view sexually explicit material including pictures, stories, and videos. Some of this material is posted on web sites where there is an attempt to verify the user's age and/or a requirement for users to enter a credit-card number on the presumption that children do not have access to credit-card numbers. Other areas on the Internet make no such effort to control access. Nevertheless, consider monitoring your credit-card bills for such charges. In addition to "adult" pornography, there are also areas on the Internet that contain illegal child pornography. If you or your children come across this type of material, immediately report it to the National Center for Missing & Exploited Children's CyberTipline® at [www.cybertipline.com](www.cybertipline.com).

Some online services and ISPs allow parents to limit their children's access to certain services and features such as adult-oriented "chatrooms," bulletin boards, and web sites. There may be an area just for children where it is less likely for them to stumble onto inappropriate material or get into an unsupervised "chatroom." At the very least, keep track of any files your children download to the computer, consider sharing an E-mail account with your children to oversee their mail, and consider joining them when they are in private chat areas.

In addition there are ways to filter or control what your children can see and do online. One type of filter, called a "spam" filter limits unsolicited E-mail including mail promoting sexually explicit material. Some ISPs and E-mail services include filters as part of their service but, if not, there is software you can purchase that will attempt to limit the type of mail that gets through.

There are also ways to filter what a child can see on the world wide web. Check with your service provider to see if they offer age-appropriate parental controls. If not consider using a software program that blocks chat areas, newsgroups, and web sites that are known to be inappropriate for children. Most of these programs can be configured by the parent to filter out sites that contain nudity, sexual content, hateful or violent material or that advocate the use of alcohol, drugs, or tobacco. Some can also be configured to prevent children from revealing information about themselves such as their name, address, or telephone number. You can find a directory of these filtering programs at www.getnetwise.org/ tools.  MSD uses such filtering software for our campus computers.

Another option is to use a rating system that relies on web-site operators to indicate the nature of their material. Internet browsers can be configured to only allow children to visit sites that are rated at the level that the parents specify. The advantage to this method is that only appropriately rated sites can be viewed. The disadvantage is that many appropriate web sites have not submitted themselves for a rating and will therefore be blocked.

While technological-child-protection tools are worth exploring, they're not a panacea. To begin with, no program is perfect. There is always the possibility that something inappropriate could "slip through" or something that is appropriate will be blocked.

Finally, filtering programs do not necessarily protect children from all dangerous activities. For example some do not control instant messaging or chat services which are particularly dangerous because they put a child in instant communications with other people. Also some filters do not work with peer-to-peer networks that allow people to exchange files such as music, pictures, text, and videos. These peer-to-peer networks are sometimes used to distribute pornography, including child pornography. <u>Filters are not a substitute for parental involvement</u>. Regardless of whether you choose to use a filtering program or an Internet rating system, the best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your children while they're online. Have them show you what they do, and ask them to teach you how to use the Internet or online service. You might be surprised by how much you can learn from your children.  If they have arranged a meeting with an Internet friend, make the first one in a public place and be sure to accompany your child.

<u>Set reasonable rules and guidelines for computer use by your children.</u>  By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to:

- Never give out identifying information — home address, school name, or telephone number — in a public message such as chat or newsgroups, and be sure you're dealing with someone both you and your children know and trust before giving out this information via E-mail. Think carefully before revealing any personal information such as age, financial information, or marital status. Do not post photographs of your children in newsgroups or on web sites that are available to the public. Consider using a pseudonym, avoid listing your child's name and E-mail address in any public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used.

- Get to know the Internet and any services your child uses. If you don't know how to log on, get your child to show you. Have your child show you what he or she does online, and become familiar with all the activities that are available online. Find out if your child has a free web-based E-mail account, such as those offered by Hotmail and Yahoo!®, and learn their user names and passwords.

- Never allow a child to arrange a face-to-face meeting with someone they "meet" on the Internet without parental permission. If a meeting is arranged, make the first one in a public place, and be sure to accompany your child.

- Never respond to messages that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your ISP, and ask for their assistance. Instruct your child not to click on any links that are contained in E-mail from persons they don't know. Such links could lead to sexually explicit or otherwise inappropriate web sites or could be a computer virus. If someone sends you or your children messages or images that are filthy, indecent, lewd, or obscene with the intent to abuse, annoy, harass, or threaten you, or if you become aware of the transmission, use, or viewing of child pornography while online immediately report this to the National Center for Missing & Exploited Children's CyberTipline at 1-800-843-5678 or www.cybertipline.com. Set reasonable rules and

guidelines for computer use by your children.

- Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.

- Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be careful about any offers that involve you going to a meeting, having someone visit your house, or sending money or credit-card information.

- Set reasonable rules and guidelines for computer use by your children. Discuss these rules and post them near the computer as a reminder. Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child's <u>excessive use of online services or the Internet, especially late at night, may be a clue that there is a potential problem</u>. Remember that personal computers and online services should not be used as electronic babysitters.

- Check out blocking, filtering, and ratings applications. Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends. If your child has a cellular telephone, talk with him or her about using it safely. The same rules that apply to computer use, also apply to cellular telephones.

There have been some highly publicized cases of exploitation involving the Internet, but that doesn't mean that every child will experience major problems. The vast majority of people who use the Internet do not get into serious trouble.

Many people, including children, have been confronted with material that is disturbing or inappropriate. There are steps parents can take to try to shield their children from such material, but it's almost impossible to completely avoid all inappropriate material. Sadly there are some cases where children have been victimized by serious crime as a result of going online. Parents can greatly minimize the chances that their children will be victimized by teaching their children to follow the safety rules on the back cover. **The fact that crimes are being committed online, however, is not a reason to avoid using these services.** To tell children to stop using the Internet would be like telling them to forgo attending school because students are sometimes victimized or bullied there. A better strategy would be to instruct children about both the benefits and dangers of "cyberspace" and for them to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

MSD is committed to working with you to ensure that our children can take advantage of the many resources on the Internet in a positive and safe manner.

*Barbara Garrison*